Cryptographic Protocol Analysis and Verification

NSA

Technical Director: Ed Zieglar

Team 1

January 28, 2022

THE UNIVERSITY OF
ALABAMA IN HUNTSVILLE

Team Members:

Evan Dow - Ashley Mahoney - Nawal Smith - Daniel Stricklin - Andrew Webb - Jordan Wilson

Faculty:

Dr. Jeffrey Kulick

1.0 Project Summary Page

Cryptographic Protocol Analysis and Verification

January 22, 2022

Investigators:

Evan P Dow - UAH - ed0034@uah.edu

Ashley L Mahoney - UAH - ak0018@uah.edu

Nawal B Smith - UAH - nbs0010@uah.edu

Daniel R Stricklin - UAH - ds0136@uah.edu

Andrew D Webb - UAH - adw0022@uah.edu

Jordan N Wilson - UAH - jnw0027@uah.edu

Field of Research: Identifying security flaws in cryptographic protocols

Keywords: Cryptographic, Analysis, Verification, Protocol, GNAP, CPSA, Haskell

Project Description: The project will be focused on the analysis and verification of the Grant Negotiation and Authorization Protocol (GNAP) and investigation of any discovered security flaws. The tool being used to perform the analysis will be the Cryptographic Protocol Shapes Analyzer (CPSA). By interpreting the shapes generated by the CPSA tool weaknesses within the protocol may be pinpointed and a solution can be found to resolve those weaknesses.

Responsibilities:

Evan Dow - Research and Development, Technical POC

Ashley Mahoney - Project Manager, documentation lead, planning, EasyChair/bid submissions, Submissions on behalf of the group, Research and Development

Nawal Smith - Meeting host/creator, Research and Development

Daniel Stricklin - Research and Development

Andrew Webb - Research and Development

Jordan Wilson - Research and Development

Budget: There is currently no set budget since the tool and research articles utilized are free. Team members are expected to work on average 8 hours per week on project tasks.

Deliverables:

- Project proposal
- Weekly INSuRE Hub progress reports
- Bi-Weekly Reports to Technical Director
- Mid-term progress report
- Mid-term presentation
- Final report
- Final presentation
- Technical report on the analysis of the GNAP

2.0 Executive Summary

Cryptographic Protocol Analysis and Verification

January 22, 2022

Investigators:
Evan P Dow - UAH - ed0034@uah.edu
Ashley L Mahoney - UAH - ak0018@uah.edu
Nawal B Smith - UAH - nbs0010@uah.edu
Daniel R Stricklin - UAH - ds0136@uah.edu
Andrew D Webb - UAH - adw0022@uah.edu
Jordan N Wilson - UAH - jnw0027@uah.edu

Keywords: Cryptographic, Analysis, Verification, Protocol, GNAP, CPSA, Haskell

Summary: The design of Cryptographic protocols matters more than ever in a society that relies on computer networks to constantly disperse sensitive information safely. Cryptographic protocols are supposed to provide the necessary security properties needed to provide key distribution, while authenticating and keeping information secret. However, many cryptographic protocols are not fulfilling their intended purpose. To help mitigate this issue, research in the application of tools that analyze cryptographic protocols is needed to affirm their authentication and secrecy properties. It is vital to not only verify the security properties of a cryptographic protocol, but also analyze the strengths and weaknesses of the tools and their usability. The purpose of this proposal focuses on the analysis and verification of the Grant Negotiation and Authorization Protocol (GNAP). A protocol that allows software to request delegated authorization to resource servers as well as request direct information. [5] Although many refer to GNAP as "the next generation of OAuth" it is not meant to be directly compatible, but instead seeks to provide functionality and solve use cases that OAuth2.0 cannot easily or cleanly address. [5] By utilizing the CPSA tool to conduct a formal analysis of this protocol we can use the generated shapes to infer weaknesses or security flaws that will provide a way to solidify the implementation. CPSA differs from other tools in that it aims to give a complete characterization of possible executions, independent of any specific security property to confirm or contradict. [1]

3.0 Motivation

This project was chosen collectively between team members because we realize the impact that cryptography has on our everyday lives whether it be simply browsing the web or even monetary transactions. The results of our analysis will significantly contribute to the success of future implementations of the GNAP which has the potential to change the authorization framework to a more generalized format. What makes this work challenging is to conduct such an analysis knowledge of the underlying protocol as well as the tool being used is required to produce adequate results.

4.0 Previous Work

The Grant Negotiation and Authorization Protocol (GNAP) is a new protocol that is intended to replace OAuth 2.0, which is the current protocol framework that is widely used in our current systems to make authentication and authorization across applications easier. It was introduced back in 2012 and is still widely used today. However, OAuth does have security vulnerabilities, so GNAP was developed to overcome those limitations however it is still in the development phase and needs to be analyzed and verified for security and flaws.

There is only one previous work that was done to analyze GNAP specifically, which was published by the University of Gothenburg in Sweden. The work is called "Security Analysis of Attack Surfaces on the Grant Negotiation and Authorization Protocol" by Åke Axeland and Omar Oueidat. This work was done to test GNAP against legacy attacks such as Cross-Site Request Forgery attacks, vulnerability Redirect URL, Access code hijacking, and "AS mix-up attack" which focuses on manipulating the authorization grant flow as a whole. This analysis was done by using a penetration testing website called portswigger. The study concluded that the GNAP is vulnerable to "AS mix-attack", and more analysis needs to be done to uncover more vulnerabilities.[1]

Our project will be different from the previous work because we are going to use a different tool called the Cryptographic Protocol Shapes Analyzer (CPSA). The CPSA is a tool that will allow us to automate the analysis and generate possible executions of the protocol known as shapes. By enumerating these shapes, we may ascertain whether they all satisfy a security condition such as an authentication or confidentiality property. We may also find other anomalies, which are not necessarily counterexamples to the security goals, such as involving unexpected participants, or involving more local runs than expected. [2] One proposed way to deal with security flaws in cryptographic protocols is through continuous verification. Verification tools should be used at early stages and repeatedly throughout the design process. The output of verification tools, such as CPSA, offers intuition (usually within seconds) that can help to identify issues and possible solutions. [4]

Gavin Lowe performed an analysis on the Needham-Schroeder (NS) protocol using the CPSA in a similar manner to the way we will be analyzing GNAP. The dashed arrow in Figure 1 reveals that the initiator and responder agree on all the values except for b.

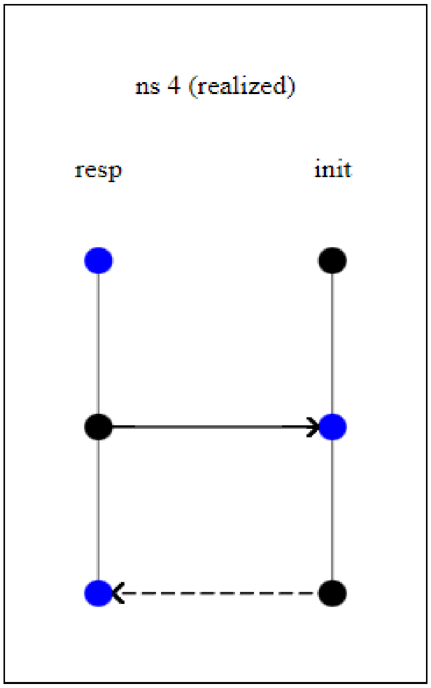

Figure 1: Initial Needham-Schroeder Analysis

This is due to the nature of the NS protocol before Lowe's analysis. The earlier NS protocol involved the following steps:

1. The Initiator (A) sends a message to the Responder (B) that contains a nonce (n1) and A's name. This message is encrypted with B's public key.
2. B responds to A with a message containing n1 and a new nonce (n2) encrypted with A's public key.
3. A responds to B with a message containing n2 encrypted with B's public key.

Lowe found that if B responded with his name in addition to the nonces in step 2, B's name could be confirmed by both entities. When reanalyzed with CPSA, the shape in Figure 2 is produced. The solid line confirms that both entities know B. This has removed the possibility of an attacker falsifying authentication messages. [6]

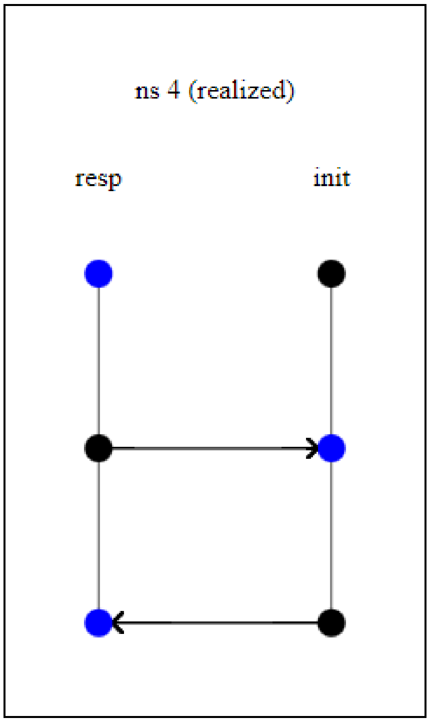

Figure 2: Needham-Schroeder Analysis Post Fix

5.0 Specific Aims

The team shall employ the CPSA to perform a cryptographic analysis of the GNAP. If any flaws are found in GNAP, the team shall investigate and propose solutions to better the protocol. The results of this analysis and potential investigation shall be used to write a report on the state of GNAP. The team should perform these tasks in a way that is presentable to the Internet Engineering Task Force (IETF) to help improve and verify the GNAP.

6.0 Plan

To effectively employ the CPSA we will dedicate a large portion of initial resources to familiarizing the team with the tool and GNAP. This will allow our investigation of GNAP to be conducted diligently to allow for any possible executions of the protocol to be verified, and for us to propose solutions to any identified security flaws. These potential solutions will have allocated research time if necessary. The results generated through the CPSA known as shapes will be key figures used in establishing a proper report as well as other research and investigation results. Throughout the entire process we shall operate cohesively as a unit to help individuals better understand the most efficient way of presenting our findings to the IETF community which will contribute to the continued success of the GNAP.

7.0 Deliverables

The team shall deliver the following items:

- Project proposal
- Weekly INSuRE Hub progress reports
- Bi-Weekly Reports to Technical Director
- Mid-term progress report
- Mid-term presentation
- Final report
- Final presentation
- Technical report on the analysis of the GNAP

8.0 Issues

The main difficulty stems from the inexperience of group members with the CPSA tool as well as the GNAP being a fairly recent development when compared to existing cryptographic protocols. We will combat this by investing our initial resources heavily in research as well as training provided by the UMBC Protocol Analysis Lab.

9.0 Bibliography

[1] Axeland, Å. and Oueidat, O., 2022. Security Analysis of Attack Surfaces on the Grant Negotiation and Authorization Protocol. [online] Odr.chalmers.se. Available at: <https://odr.chalmers.se/handle/20.500.12380/304105> [Accessed 23 January 2022].

[2] Doghmi, S. F., Guttman, J. D., and Thayer, F. J. "Searching for Shapes in Cryptographic Protocols" in Tools and Algorithms for the Construction and Analysis of Systems, Berlin, Heidelberg, 2007, pp. 523–537. doi: 10.1007/978-3-540-71209-1_41.

[3] Liskov, M., Rowe, P. and Thayer, F., 2022. Completeness of CPSA. [online] The MITRE Corporation. Available at:

<https://www.mitre.org/publications/technical-papers/completeness-of-cpsa> [Accessed 18 January 2022].

[4] Molina-Markham, A. and Rowe, P. D. “Continuous Verification for Cryptographic Protocol Development,” in Proceedings of the 1st ACM Workshop on the Internet of Safe Things, Delft Netherlands, Nov. 2017, pp. 51–56. doi: 10.1145/3137003.3137006.

[5] Richer, J., Parecki, A. and Imbault, F., 2022. Grant Negotiation and Authorization Protocol. [online] Gnap-core-protocol-editors-draft.netlify.app. Available at: <https://gnap-core-protocol-editors-draft.netlify.app/draft-ietf-gnap-core-protocol.html> [Accessed 22 January 2022].

[6] Liskov, Moses D., et al. *The Cryptographic Protocol Shapes Analyzer: A Manual - Haskell*. [online] The MITRE Corporation, 21 May 2020, Available at: <https://hackage.haskell.org/package/cpsa-3.3.2/src/doc/cpsamanual.pdf> [Accessed 22 January 2022].

10.0 Biographical sketches of the investigator(s)

Evan Dow is a graduate student at the University of Alabama in Huntsville pursuing an M.S in Cybersecurity with a Computer Engineering focus. He has 5 years of experience in the engineering field and currently works as a software engineer in Huntsville. He received his B.S. in Computer Engineering from the University of Alabama in Huntsville in May of 2019. He has experience in network programming and distributed computing. Evan plans to use his master’s degree to pursue a career in Computer Engineering with a focus on red teaming and cryptography. Evan’s skills include C/C++, Java, Python, and Rust programming, as well as networking tools such as Wireshark and Nmap. He is experienced using the Bash shell as well as the Linux kernel.

Ashley Mahoney is a graduate student at the University of Alabama in Huntsville. She has completed her undergraduate degree in Information Systems with a focus in Cybersecurity and was a Scholarship for Service (SFS) recipient. Ashley is CompTIA Security+ certified and currently works for the Center for Cybersecurity Research and Education (CCRE). Through CCRE she has taught and created Cybersecurity related curriculum for teachers and educated deaf and hard of hearing students as well as visually impaired students and has moderate knowledge of American Sign Language (ASL). She also works part time with DEVCOM AvMC as a supply chain analyst doing research and training. Ashley's skills include basic scripting, digital forensics tools, Wireshark, Autopsy, Amazon AWS, networking, network security and defense, Linux operating system, technical writing, virtualization, micro controllers, and education with a focus in Cybersecurity.

Nawal Smith is a graduate student at the University of Alabama in Huntsville pursuing a Master's in Cybersecurity Management, with an undergraduate degree in Information Systems-Cybersecurity. Nawal is a Scholarship for Service recipient and CompTIA Security+ certified. She has been an intern at the University of Alabama in Huntsville (UAH) Center for Cybersecurity Research and Education Center (CCRE) since May 2019. Through CCRE UAH, she assisted in researching a wide variety of cybersecurity related topics including solving a variety of the National Institute of Standard and Technology NIST (National Initiative for Cybersecurity Education Challenges) NICE Challenges and documented solutions and findings.. Last summer, Nawal was an intern at the Cybersecurity Infrastructure Security Agency CISA, she gained experience researching Industrial Control Systems ICS vulnerabilities using Shodan and Censys and other open source tools to score vulnerabilities and proactively notify owners of their cybersecurity risk through CISA's administrative subpoena process. Furthermore, she developed a Cybersecurity Risk Lexicon to standardize common terminology used within vulnerability management analytic products. Nawal's skills include network and system administration, Linux, CISCO IOS, MySQL workBench, Amazon AWS, Python, Network Defense, digital forensics, NIST Risk Management Framework, WordPress, penetration testing, and virtualization.

Daniel Stricklin is a Master's student in CyberSecurity at the University of Alabama in Huntsville. He is employed full-time at Cullman Electric Cooperative as their Manager of Information Technology for the last 20 years. He has taken a variety of network, security, programming and management classes during the course of his undergraduate and graduate degrees. Some of his skills include networking, system administration, security, C++ programming, digital forensics, implementing, monitoring and maintaining network architecture and ERP systems, designing policies, procedures, and documentation, and managing various compliance related requirements, data mining, research and reporting. Daniel is CompTIA Security+ certified and his goal is to continue to develop and enhance his knowledge in CyberSecurity so he can apply that knowledge to protecting the assets within the organization where he works.

Andrew Webb is a graduate student at the University of Alabama in Huntsville, pursuing a degree in Cybersecurity. He is employed full-time at the University of Alabama in Huntsville Systems Management and Production Center. Through the UAH SMAP Center he has worked on contracts for the United States Space and Missile Defense Command which include development of small satellite technologies as well as designing a Graphical User Interface for an antenna tracking system. These opportunities as well as Computer Science Undergraduate classwork have allowed him to learn skills that include various programming languages such as C, C++, C#, Python, and Bash scripting, experience with the Linux operating system, quasi-embedded flight software, GUI application development, Qt framework, MySQL databases, Wireshark, virtual machines, x86 and Advanced Reduced Instruction Set Machine architectures, some networking and Risk Management Framework processes, and hardware interfaces such as Ethernet, RS-422 Serial, Serial Peripheral Interface, Inter-Integrated Circuit, and Universal Serial Bus. In addition to the projects listed above he also picked up a personal contract on the side which allowed him to further develop skills in embedded software development as well as learn about Wi-Fi Direct and Bluetooth applications.

Jordan Wilson is a graduate student at the University of Alabama in Huntsville pursuing her M.S. in Cybersecurity Management. She has four years of experience in the Information Technology sector and currently is employed through the Center for Cybersecurity Research and Education (CCRE) where she is helping to build out a national Cybersecurity curriculum for secondary education. A few of the skills she possesses, but are not limited to are report writing, research development, structuring presentations, technical writing, and use of digital forensics. She is CompTIA Security+ certified.

11.0 Schedule

Milestone	Expected Completion Date	Due Date
Bid Submissions	January 18th, 2022	January 18th, 2022
Proposal Submission	January 27th, 2022	January 28th, 2022
CPSA Installation	January 27th, 2022	February 1st, 2022
CPSA Manual Review	February 3rd, 2022	February 4th, 2022
CPSA Training	February 8th, 2022	February 10th, 2022
Bi-Weekly Report 1	February 10th, 2022	February 11th, 2022
Bi-Weekly Report 2	February 24th, 2022	February 25th, 2022
Mid-Progress Presentation Submission	March 11th, 2022	March 17th, 2022
Mid-Progress Report & Presentation (Midterm)	March 11th, 2022	March 18th, 2022
Bi-Weekly Report 3	March 31st, 2022	April 1st, 2022
Bi-Weekly Report 4	April 14th, 2022	April 15th, 2022
Final Presentation Submission	April 26th, 2022	April 28th, 2022
Final Report & Presentation	April 27th, 2022	April 29th, 2022

12.0 Budget

We anticipate using only free resources from published authors.

Each group member will need to dedicate eight hours of their time a week to working towards an implementation of the Grant Negotiation and Authorization Protocol (GNAP) using the Cryptographic Protocol Shapes Analyzer (CPSA) tool. We anticipate using only open-source software development environments to implement the protocol. We will also require time commitments and periodic assistance from our professor and mentor within the INSuRE program.

Resource	Cost
Direct Costs:	
Time	$0
CPSA Tool	$0
GNAP Protocol	$0
Open-source software	$0
Indirect Costs:	
University Overhead Costs	$0
Total Costs:	$0

13.0 Appendix A: Research Conference

Our thesis could be published in the Internet Engineering Task Force (IETF) data tracker platform. We believe this will be the perfect conference because it directly supports the GNAP Development and implementation through working groups. It is also an international community of researchers, network designers, and vendors who work to make the internet operation smoother and anyone with technical skills who is willing to contribute can join.

14.0 Broader Impact

A formal analysis of GNAP will provide the IETF with a verification of the protocol or a solution to any weaknesses. This information will give the IETF a path forward regarding GNAP, and will help move the protocol towards being accepted.